RSA Token Login

Updated 10/24/15

For all RSA RDHPCS bastion authentication Logins: Gaea, Theia, Jet

About Authentication

We are in the process of transitioning from RSA authentication to CAC authentication. This section is for those users are not required to login via CAC. See: Logging in

We currently have three (3) NOAA RDHPCS systems that are available to the user community. Depending on which project(s) you are on, will dictate which system you will have the abililty to logon.

RDHPCS uses multiple authentication mechanisms, to ensure secure access to NOAA resources. Having multiple methods also provides flexibility in interacting with the systems, depending on the use case.

- The **one-time password token** (RSA Token) provided to you after you have applied for your account is used to initiate logins from outside the system.
- **X.509 RDHPCS certificates** are used within the system to authenticate between resources. The X.509 certificates are created using a user-defined pass-phrase. A validated certificate stays valid for a set period of time (currently 30 days). You do not have to re-validate your certificate every time you login to the system.

For more information, please see: Information about X.509 RDHPCS Certificates

The RSA login process

- Use an SSH client to login

```
ssh User.Name@host name
```

Where User.Name is your RDHPCS logon name (your NOAA NEMS name: ex.: John.Smith), and “host name” is system host name for the bastion your are logging in through from the table below.

The RSA passcode is your RSA token pin followed by the current 6 numbers displayed on the RSA token. (ex. if your pin is “123abc” you would enter 123abcXXXXXX where XXXXXX is the current 6 numbers on your RSA token. The 6 numbers on the token must still be displayed when you press enter or access will be denied.

Host Names:

There are two possible paths to get to each RDHPCS system. The one goes through Boulder, CO, and the other one is through Princeton, NJ. So depending on your location you may want to choose an appropriate primary path, but you should be ready to use the other path if your primary bastion is

down. Current RSA host names to the bastions will change on 11/01/16 per the tables below.

Prior to 11/01/16 the current RSA host names will work for RSA login:

```
* Jet logins *
Boulder bastion:     jet.rdhpcs.noaa.gov
Princeton bastion:   jet.princeton.rdhpcs.noaa.gov

* Theia logins *
Boulder bastion:     theia.rdhpcs.noaa.gov
Princeton bastion:   theia.princeton.rdhpcs.noaa.gov

* Gaea logins *
Boulder bastion:     gaea.rdhpcs.noaa.gov
Princeton bastion:   gaea.princeton.rdhpcs.noaa.gov
```

Starting 10/24/16 the following RSA host names will work for RSA login:

```
* Jet logins *
Boulder bastion:     jet-rsa.boulder.rdhpcs.noaa.gov
Princeton bastion:   jet-rsa.princeton.rdhpcs.noaa.gov

* Theia logins *
Boulder bastion:     theia-rsa.boulder.rdhpcs.noaa.gov
Princeton bastion:   theia-rsa.princeton.rdhpcs.noaa.gov

* Gaea logins *
Boulder bastion:     gaea-rsa.boulder.rdhpcs.noaa.gov
Princeton bastion:   gaea-rsa.princeton.rdhpcs.noaa.gov
```

- If your certificate is valid, it will be re-validated (no pass-phrase necessary) and then you will be logged into the R&D HPC system.
- If your certificate has expired, you will be asked to validate your certificate using your pass-phrase.
- If you have no certificate (never logged in before), you will be prompted to create one.
- After authenticating with your token, you will be asked to create a certificate and specify a pass-phrase.
- The certificate then must be signed by a HPC administrator.
- **Signing a certificate may take up to one business day.**

Example of RSA token authentication

```
$ ssh John.Smith@jet-rsa.boulder.rdhpcs.noaa.gov
The authenticity of host 'jet-rsa.boulder.rdhpcs.noaa.gov (XXX.XXX.XXX.XXX)'
can't be established.
RSA key fingerprint is XXX:XXX.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'jet-rsa.boulder.rdhpcs.noaa.gov,XXX.XXX.XXX.XXX'
```

```
(RSA) to the list of known hosts.
**********************************************************************
*                                WARNING!                            *
**********************************************************************
* This is a United States Government computer system, which may be      *
* accessed and used only for official Government business by authorized *
* personnel. Unauthorized access or use of this computer system may     *
* subject violators to criminal, civil, and/or administrative action.   *
*                                                                       *
* All information on this computer system may be intercepted, recorded, *
* read, copied, and disclosed by and to authorized personnel for        *
* official purposes, including criminal investigations. Access or use   *
* of this computer system by any person, whether authorized or          *
* unauthorized, constitutes consent to these terms.                     *
**********************************************************************
Access is via First.Last username only. Enter RSA PASSCODE:
```

At this point is where you enter your PIN appended with the one-time password generated by your token.

Successful token authentication will be followed by:

```
Last login: Thu Dec 1 17:15:31 2011 from XXX.XXX.XXX.XXX
Welcome to the NOAA RDHPCS.
```

Example of certificate and passphrase generation, when logging in for the first time

```
Certificate unavailable, falling back to token access.

Hello John Smith!

Access to NOAA R&DHPCS resources require use of digital certificates.
You will have two certificates: a "master" and a "proxy". As this may
be the first time that you are using certificates, the process has been
automated as much as possible.

A very simple way to think of certificates is that your "master"
certificate is like a passport. A passport is necessary before you
travel and identifies you. It will be renewed on an infrequent basis,
\and is issued, or signed, by a central authority. The "proxy"
certificate is your visa. It defines where you can go and how long
you can stay. They last for a relatively short period of time and
need to be renewed often.

Proxy certificates are used by yourself to access certificate-aware
systems and by programs on your behalf, such as batch jobs and data
transfers that are "running as you." R&DHPCS Proxy certificates are
good for 30 days. For the R&DHPCS systems, every time you log in
```

```
through this bastion host, the system will automatically renew your
proxy certificate so that it will not expire for 30 days from that log in.

You are about to generate a 'master' certificate, good for one year,
which will be used to generate your proxy certificates. This master
certificate is protected by a passphrase, which you need to choose
now. Try to choose a sentence, or phrase, that you will be able to
 remember even if you do not use it frequently. Once your certificate
has been signed (usually 1-2 business days), the next time you log in,
you will be asked to enter this passphrase, along with your password
from your token card -- these steps create a proxy certificate that
will be used for access.
```

Now you will be asked to enter and verify a passphrase for your certificate.

IMPORTANT: It is important to remember this pass phrase.

- The system will prompt you for your pass phrase if you have not logged in for extended periods of time.
- The system will prompt you for you pass phrase if your master certificate is approaching its expiration.

If you forget your pass phrase you will have to regenerate the certificate. This may interrupt your ability to use the system because you will have to wait for your certficate to be signed.

```
Please enter a certificate passphrase; at least 3 words:
Please confirm the passphrase:
```

NOTE: If entered incorrectly, you can try again but the prompt may change to looks like this:

```
Passphrase must be at least three words
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Successful certificate generation will be followed by:

```
Certificate request successfully generated.
Your certificate should be signed and available for use in a business day.
```

At this point you can hit ctrl-c and end the login process. **You will not be able to access the system until the certificate has been signed.**

You will receive email confirmation when it is completed, which will have a subject similar to:

```
Signed: NOAA RDHPCS Certificate for John.Smith@noaa.gov
```

Example of proxy cert generation, after you have a new (signed) cert

SSH to a R&D HPC system as specified above and authenticate as in the [Example of RSA token authentication].

```
$ ssh John.Smith@jet-rsa.boulder.rdhpcs.noaa.gov
**************************************************************************
*                                WARNING!                                *
**************************************************************************
* This is a United States Government computer system, which may be       *
* accessed and used only for official Government business by authorized *
* personnel.  Unauthorized access or use of this computer system may     *
* subject violators to criminal, civil, and/or administrative action.    *
*                                                                        *
* All information on this computer system may be intercepted, recorded, *
* read, copied, and disclosed by and to authorized personnel for         *
* official purposes, including criminal investigations.  Access or use  *
* of this computer system by any person, whether authorized or           *
* unauthorized, constitutes consent to these terms.                      *
**************************************************************************
Access is via First.Last username only. Enter RSA PASSCODE:
```

Enter your PIN+token as instructed.

```
Creating directory '/home/John.Smith'.
Last login: Fri Dec  2 21:19:18 2011 from XXX.XXX.XXX.XXX
/usr/bin/xauth:  creating new authority file /home/John.Smith/.Xauthority
Welcome to the NOAA RDHPCS.

No proxy certificate found, generating.
Expired or nonexistent proxy certificate.
Please enter your certificate passphrase:

Warning: your certificate and proxy will expire Sat Dec  1 17:25:24 2012
 which is within the requested lifetime of the proxy
Proxy certificate initialization complete.
Wait for the tokencode to change,
then enter PIN + the new tokencode:
```

Enter your PIN+token as instructed.

```
Proxy certificate retrieved.
You will now be connected to OneNOAA RDHPCS: Jet system
Hit ^C within 5 seconds to select another host.
```